International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

Security for Cloud Connectivity

Nagesh R

UG Student, Dept of ECE, RV College Of Engineering, Bangalore, Karnataka, India

---

Abstract - *The last two decades have witnessed a tremendous revolution in the computational systems. There has been a changeover from the centralized systems to the newly modeled distributed technology. The changes developed have been enhanced by the emergence of virtualization technology that has in turn facilitated the diversity in system architecture to a more advanced virtual centralization. The two structures, centralized computing, and virtual centralization have significant distinctions that have put the two systems into a test to establish a common ground for the best next generation technology. Unlike centralized computing where the end user has complete control over data and processes, virtual centralization entails access to data that the client does not know neither the location of the data nor the processing center for the accessed information. The client has to receive data from a centralized storage location with the use of a unique identification, password, decryption code and other security authentication modules. The traffic and dynamics involved in acquiring information in such a model are quite complex, and this may pose a security threat to the users. Information can and may be intercepted at the network level, host end, application employed in access or even the data level. Centralized computing has a limited number of services that makes securing the systems easier and as per the client's requirements. The existence of diversity makes developing conventional security models quite a challenge. The implementation of different servers with unique authentication code depending on the importance of the data involved may be a solution to the insecurity menace. The paper focuses on securing the cloud data and access through the proposed model as cloud computing is the next big thing in the computing world and the future of computers and data access.*

Key Words: Cloud Computing, Connectivity, Security, Cloud Architecture, Reliability

1.INTRODUCTION

Information security has been a major challenge ever since the internet came into play. Hackers have become more aggressive, and the world's expenditure on system security and the cyber-crime contention department has been on the rise with the graph bearing an exponential trend[11]. As much as there were insecurity issues with the centralized systems, users could easily trust their systems as opposed to the implementation of the new technology-cloud. Most internet users and multinational companies that have been reluctant to adapt to the new system may be considered paranoid, but their argument or reasoning may make much sense. Computer users stored their data in their hard drives at home or in office and protected them with super long passwords but yet perpetrators in one way or the other could still get their hands on sensitive data[7]. It could only get worse now that the storage location is not defined, and the access method is through the same internet that could not protect the users from perpetrators before.

Cloud computing may be considered to operate on the same concept as 3G and higher versions of mobile networks where resources are shared by many users and are only availed during demand[3]. There is a high economic value associated with such a system although there are other challenges that may limit the convenience. The idea behind setting up a cloud connectivity lies in the fact that the processes and services being executed by any computational system at the clients end can be conveniently transferred to an established space or virtual station[2]. The data, processes and any other resources required by the client can then be availed dynamically for the user's consumption on demand. Of course, at this juncture, it is noticeable that the overall cost regarding storage space may be reduced in the end. Storage cost per unit of data has been high and a straining factor in technology.

All the client's data are accessed through the Internet at the user's convenience. The user can log in to the system using any device provided that the access data is correct. The mobility associated with the cloud is one of the factors that have contributed to the success of implementation of the technology. However, the internet is something that the clients have no control over whatsoever. There are millions of internet users across the globe with different aims and intentions. Being a virtual environment with metadata, cloud computing has numerous threats that are different from the ones faced by the physically centralized systems[9]. The paper examines the existing security systems, their weaknesses and ways to enhance them. The viable security systems are then compared to the proposed model to establish a common ground in

determining the best solution for an air-tight cloud storage and data access.

2. Cloud Computing Architecture

A comprehensive understanding of the cloud connectivity security system and operation demands a solid understanding of the architecture. Information flow between the server and the client and the various dynamics governing such communications. The security of any communication network relies on how safe the information is from the source to the destination and the degree of ease of intercepting such data[12].

2.1 Data Security in Cloud

Security in cloud technology is used to refer to the guaranteed degree of confidentiality for a given set of information stored in digital form. Companies and individuals have great ideas and some dirty work or information that they may want to prevent from getting into the wrong hands[1]. Today that the data are kept in a centralized location makes users more worried than in the past. Any leeway to accessing the data stored in the cloud may mean serious damages to individuals and industries. Most people prefer keeping their data and confidential in the cloud as opposed to mobile gadgets like tablets, laptops, and mobile phones[8]. These devices are prone to theft and can be easily used to acquire an individual's information or data.

Security in cloud exists at two different levels, the public cloud, and the private cloud. The two can also be categorized as the server end and the client end. There exist the aspect of the network, but that will be covered under the server end. Hackers may be more inclined to attack from the public cloud as opposed to the private cloud[6]. As much as there is a lot of important data stored in the cloud, organizations and individuals may consider making their private networks impenetrable[3]. Protecting private networks is quite easier by employing firewalls and other tight security measures that will alert the users of any looming threats or malicious search. Security at the private side of the network may not be much an issue compared to the public cloud. Access of any secure system requires authentication and authorization. Any individual able to access confidential information must have authentication and authorization irrespective of the method employment to gain access to the systems. Any attempts to establish a secure system depends on the reliability and effectiveness of a system to filter and deny access of perpetrators and allow authorization of registered users only[5]. There are numerous security systems used to protect the access of data by unauthorized personnel, but there are still loopholes. The existence of loopholes on some of these systems forms the basis of this paper.

Database injection is the most common access technique that has been employed by hackers to gain access to unauthorized data. Cloud may be considered as a pool of metadata within a centralized system that is accessed by some users whose identity, authentication and authorization are stored in some centralized database[10]. If a hacker can incorporate a user name and a password in the system, they can conveniently gain access to data and allocate themselves administrator privileges that will allow them to access a lot of data with ease. Malicious software can be used to trick users into clicking a link that will warrant perpetrators a lee way into accessing the data. An air-tight security system is required to ensure that information is safe and remain confidential at all times.

3. Reliability of Cloud and the Security System Employed

Security is a major issue in cloud computing, and all informed computer and internet users are aware of this fact. Enhancement of security should, however, not tamper with the ease of data access and reliability of the system. It is because of factors such as fast and mobile access that got people to trust and invest in the technology in the first place[12]. Making data access almost impossible to users in the name of securing the system may beat the logic of having cloud technology in play.A high level of integrity is required for data stored in the cloud. The systems must ensure a complete transaction and authenticity of any given process. Just like in a banking system, the cloud should be structured to ensure that a transaction or an access process goes to completion or does not occur at all. By so doing, there will not exist incomplete transactions or processes that may warrant the system unauthentic. Storage, as mentioned earlier, is quite expensive, and users will only store the data they consider very important in cloud and integrity is by far a determining factor in running the systems.

Integrity, reliability and availability of data to users may be part of the security structure of cloud technology, but these are solely the duty of the service providers. Customers pay a lot of money to ensure that their data are securely stored and availed upon their demand. Cloud technology can be compared to the mobile phones and the network provided by various service providers around the globe. Mobile phones may be considered as the client end with the BSC, BSS and MSC treated as the server size[5]. Clients will always have their mobile phones and connection for communication is only established during a

request for connection. During this period, the resources are engaged, and customers are charged for the total time spent accessing the resources. The cost of maintaining such systems is a collective responsibility and does not overwhelm any single individual. Anyone who can comprehend the operation of mobile systems is better placed to visualize the operation of the cloud technology. Lack of integrity, reliability and availability of data and resources can be conveniently compared to the inconveniences offered once in a while by the mobile system that are widely in use today.

4. The Proposed Idea

Service providers may implement the divide and manage rule to ensure the best security for their clients. According to current status, data about a particular service or company are stored in the same pool. What this means is that confidential data may be stored in the same location irrespective of the level of confidentiality required for the given set of data. Service providers may consider coming up with measures to categorize the data according to the level of importance and provide the necessary security. Resources used for storing sensitive data can be protected by a high level firewall and access restricted to the few individuals that have the authorization for access of such information. Unlike the current authorization and authentication models used, the proposed security system will require a unique code to access a particular cloud resource. Codes are assigned to users based on how much they are willing to pay to ensure the safety of their data. Resource identification codes will enable users to be divided into categories that are manageable regarding securing and managing the data presented.

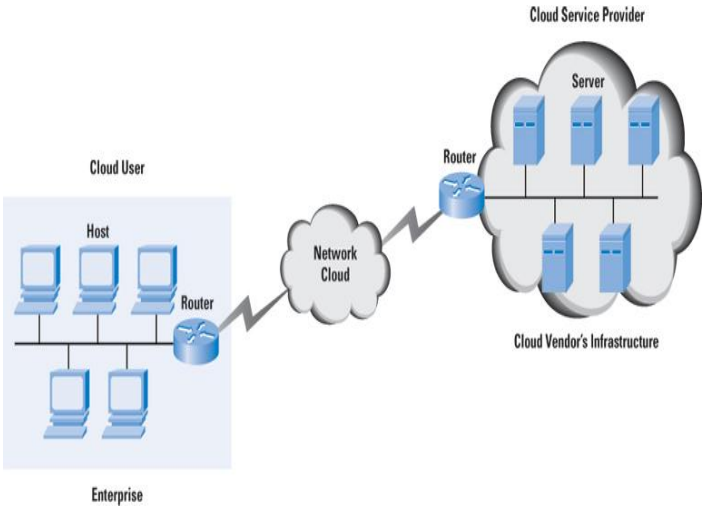

Fig -1 : Cloud computing model

Cloud resources used for the storage of sensitive data can be put under a tight surveillance by the service provider. Any encroachment by unidentified users leads to immediate action, and when the threat proves too serious, the entire system is shut down to minimize the slightest chance of perpetrator's access to sensitive data. The codes used for resource identification can be encrypted such that hackers and attackers do not get any opportunity of acquiring such information through malware or any other way around the systems. The early stages of security enhancement using this system should involve encrypted resource identification codes to determine how that works out. Figure 1 shows the typical cloud technology and the conventional method of their operation and management by the service providers. It is evident that all users have access to the same resources and databases. The divide and manage approach locate different resources to different users. Devices have to login to the servers before being invoked to enter user name and passwords. There will be minimal or no chances of accessing protected data because there is no sharing of databases among different entities.

Should the divide and manage approach prove fruitful, biometrics can be incorporated to enhance further security. It is important to note that this model does not deal with user authentication, but rather resource identification. The system is intended to identify a specific resource that contains the user's data. Succinct identification of the resource then allows the subscriber to login into the system using the username, password and a unique code that is automatically integrated into the user access codes upon identification of the right cloud resources.

4.1 Challenges of the Proposed Idea

The cost of setting up a cloud system is quite high, and separating resources may strain the service providers economically. Securing each module on its own may call for more resources and increased muscle regarding manpower. As much as cloud connectivity is about pooling resources and enhancing connectivity, the cost may be too much for the clients to bear. The world's economic situation is slightly off the hook, and serious elevation in operation cost may end up scaring potential users away. It would, however, be recommended that individuals with the ability to afford such services invest in them because the cost of recovery upon encroachment is nothing close to the amount that would have been involved in ensuring enhanced security system.

5. Conclusion

Security is a major issue of concern in the technological world especially at a time when everything is going electronic. Cloud connectivity is one of the most embraced technologies because of the conveniences associated with the system[4]. Companies are doing as much work to enhance security, but the use of passwords and encryption at the client end are not sufficient enough to protect the metadata. The proposed separation of data and logging in

into the desired servers and cloud resources with different level of security may be a lasting solution to the insecurity associated with cloud systems. The cost of putting up separate systems for distinct users may be a hitch to the service providers, but most companies may consider this path because the cost of dealing with encroachment may be too high in the end. Having a different level of securities for distinct information is the way to handle data security and lead hackers to the direction they want. Once their activities are detected, a sure and enhanced security can be implemented for online information.

REFERENCES

[1] Bessis, N. (2012). *Technology integration advancements in distributed systems and computing*. Hershey, PA: Information Science Reference.

[2] Cindhamani, I., Punya, N., Ealaruvi, R., Dhinesh, B. L. D., & 2014 5th International Conference on Computing, Communication and Networking Technologies (ICCCNT). (July 01, 2014). An enhanced data security and trust management enabled framework for cloud computing systems. 1-5.

[3] Dhivakar, A. (2015). *A multi-level security in cloud computing: Image sequencing and RSA algorithm*.

[4] Erl, T., Puttini, R., & Mahmood, Z. (2013). *Cloud computing: Concepts, technology, & architecture.*

[5] Han, S., Xing, I., & 2011 IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS). (September 01, 2011). Ensuring data storage security through a novel third party auditor scheme in cloud computing. 264-268.

[6] International Workshop on Security. In Yoshida, M., & In Mouri, K. (2014). *Advances in information and computer security: 9th International Workshop on Security. IWSEC 2014, Hirosaki, Japan, August 27-29, 2014. Proceedings*.

[7] Khosrow-Pour, M. (2014). *Contemporary advancements in information technology development in dynamic environments*

[8] Loo, A. W.-S. (2013). *Distributed computing innovations for business, engineering, and science*. Hershey, Pa: IGI Global(701E.ChocolateAvenue, Hershey, Pennsylvania, 17033, USA).

[9] Mukhopadhyay, S. C., Jayasundera, K. P., & Fuchs, A. (2013). *Advancement in sensing technology: New developments and practical applications*. Berlin: Springer.

[10] Ruan, K. (2013). *Cybercrime and cloud forensics: Applications for investigation processes*. Hershey, PA: Information Science Reference.

[11] Saroj, S. K., Chauhan, S. K., Sharma, A. K., Vats, S., & 2015 IEEE International Conference on Computational Intelligence & Communication Technology (CICT). (February 01, 2015). Threshold Cryptography Based Data Security in Cloud Computing. 202- 207.Wang, J., & Kissel, Z. A. (2015). *Introduction to network security: Theory and practice*.

[12] Zhong and Zhen (2007). "An Efficient Authenticated Group Key Agreement Protocol." Security Technology, 2007 41st Annual IEEE International Carnahan Conference.